UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
Southern Division

CYNTHIA SCOTT, on behalf of herself and all others similarly situated, Plaintiff, vs. FLAGSTAR BANK, N.A., Defendant.	Case No. 2:23-cv-12726

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Cynthia Scott ("Plaintiff"), individually and on behalf of the proposed class and subclass defined below, brings this action against Defendant Flagstar Bank, N.A. ("Flagstar"), and alleges as follows:

I. SUMMARY OF THE ACTION

1. This action concerns Flagstar's failure to secure its customers' confidential information. For the third time in less than three years, sensitive personal information of Flagstar customers has been compromised and acquired in a major cyberattack.

2. Between May 25 and May 31, 2023, an unauthorized actor accessed Flagstar's network (the "Data Breach"). After detecting this hacking incident on

June 3, 2023, Flagstar did not report it until October 5, 2023.[1] The impacted files contained names, addresses, Social Security numbers, bank account numbers, and birthdates of approximately 837,390 customers.[2]

3. As a result of Flagstar's data security failures, Plaintiff and Class Members face a significant threat of identity theft and other harm—now and for the foreseeable future. Plaintiff accordingly seeks compensatory damages together with injunctive relief to remediate Flagstar's failure to secure her personally identifiable information ("PII"), and to provide credit monitoring, identity theft insurance, and credit repair services to protect the class of Data Breach victims from identity theft and fraud.

II. PARTIES

4. Plaintiff Cynthia Scott is a citizen and resident of Detroit, Michigan. Ms. Scott, a Flagstar customer, was notified by Flagstar of the Data Breach that occurred between May 27 and May 31, 2023. Flagstar informed Ms. Scott that one or more of the files affected by the breach "may have contained information including your name, address, Social Security number, account number, and date of birth." Among other harm, Ms. Scott suffers from distress and anxiety because

[1] https://www.cpomagazine.com/cyber-security/flagstar-bank-suffers-a-moveit-data-breach-impacting-over-800000-customers/ (last visited Oct. 23, 2023).
[2] https://apps.web.maine.gov/online/aeviewer/ME/40/a67798f0-9798-4a17-b31f-6c7d003dbfb6.shtml (last visited Oct. 24, 2023).

the Data Breach subjects her to an increased risk of identity theft, fraud, and other types of monetary harm.

5. Defendant Flagstar was chartered in 1987 as a federal savings bank. It now has assets of $31 billion and is the sixth largest bank mortgage originator, and the second largest savings bank, in the United States. Flagstar's principal place of business is located at 5151 Corporate Drive, Troy, Michigan.

III. JURISDICTION AND VENUE

6. This Court has jurisdiction over the lawsuit under the Class Action Fairness Act, 28 U.S.C. § 1332, because this is a proposed class action in which: (1) there are at least 100 class members; (2) the combined claims of class members exceed $5,000,000, exclusive of interest, attorneys' fees, and costs; and (3) Flagstar and Class Members are domiciled in different states.

7. The Court has personal jurisdiction over Flagstar because its principal place of business is within this District and it has sufficient minimum contacts in Michigan to render the exercise of jurisdiction by this Court proper.

8. Venue is proper in this District under 28 U.S.C. § 1391(b) because Flagstar is headquartered in this District and a substantial part of the events or omissions giving rise to the claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Customers Trust Flagstar With Their PII

9. Flagstar provides banking and lending services. To bank with Flagstar, individuals must provide Flagstar with their PII, including Social Security number, first and last name, address, and date of birth.

10. In Flagstar's Privacy Notice, published on its website, Flagstar represents to its customers that "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[3] Flagstar also states that it will disclose customer PII only in certain circumstances—none of which includes a circumstance like the Data Breach.

11. Flagstar also recognizes on its website that "[t]he war against cyber criminals is fought daily as attacks become more difficult to detect and stop," and there is "no way to predict the damage that can be caused by a single cyber attack."[4] Flagstar knows that "identity fraud affects 17 million people on an annual basis" and that its customers entrust it with their "data and information that is valuable to cyber criminals."

12. Flagstar advises its own customers to follow "10 cyber security tips to safeguard against potential online threats." The second of Flagstar's cyber

[3] https://www.flagstar.com/content/dam/flagstar/pdfs/about-flagstar/PrivacyPolicy.pdf (last visited Oct. 25, 2023).

[4] https://www.flagstar.com/financial-resource-center/cyber-safety.html (last visited Oct. 24, 2023).

security tips is: "update your software." Flagstar emphasizes the importance of "mak[ing] sure your programs are up to date and running the latest version."

13. Plaintiff and Class Members reasonably expected that Flagstar would keep their PII confidential and would not permit unauthorized disclosures of this information. In opening and maintaining financial accounts with Flagstar, Plaintiff and Class Members relied upon Flagstar to securely maintain their PII and to implement data security measures that would prevent its unauthorized disclosure.

14. Flagstar failed to implement reasonable data security measures and failed to take appropriate steps to protect and secure the personal information of its customers, permitting the third large breach of its electronic systems in just three years.

Flagstar's Files Are Breached by Cyber Criminals

15. On October 5, 2023, Flagstar began mailing notices of the Data Breach to affected persons.

16. In the letter, Flagstar disclosed that some of its customers' "personal information was disclosed to an unauthorized party" in a hacking incident.

17. Between May 25 and May 31, 2023, an unauthorized actor accessed Flagstar's network.

18. Information exposed in the Data Breach includes names, addresses,

account numbers, dates of birth, and Social Security numbers.

19. In the letter, Flagstar advised customers to take protective measures, such as reviewing accounts frequently, signing up for credit monitoring, placing fraud alerts, and requesting a credit freeze.

20. Social Security numbers and other PII are in high demand on the black market. This information commands value and is regularly sold and traded on the "dark web."

21. The loss of a Social Security number is particularly damaging because it cannot easily be changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

22. Flagstar has offered Class Members two years of credit monitoring services from Kroll. This offer is inadequate, including because it will leave Plaintiff and Class Members unprotected after two years, even though their information will still be in the hands of cyber criminals. Criminals often wait several years before using stolen data for identity theft, and once the personal information is posted online, opportunities for misuse continue indefinitely.

Flagstar's Systems Had Foreseeable Vulnerabilities

23. In December 2020 and January 2021, a legacy file transfer application used by Flagstar was breached, compromising the PII of nearly 1.5

million Flagstar customers and employees. As with the Data Breach at issue in this case, the stolen information in that earlier breach included names, Social Security numbers, account numbers, and addresses. The provider of the file transfer application, Accellion, Inc., described it as a "20 year old product nearing end-of life" and stated it had "encouraged all FTA customers to migrate to kiteworks."[5] Flagstar failed to heed these warnings.

24. Hackers also targeted Flagstar with ransom demands, posting Social Security numbers and home addresses of Flagstar employees taken in that breach.

25. Flagstar then suffered a second data breach in early December 2021 that compromised the PII of 1.5 million Flagstar customers and employees. The stolen information in that breach similarly included names, phone numbers, and Social Security numbers. Flagstar did not notify its customers of that breach until six months after it occurred, in June 2022.

26. Flagstar knew that safeguarding its customers' PII is critical. Over the past several years, data breaches like the repeat incursions into Flagstar's electronic systems have occurred and been reported on. Yet, even after being twice targeted successfully by hackers, Flagstar failed to take the defensive

[5] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last visited Oct. 24, 2023).

measures necessary to prevent the third breach that exposed Plaintiff's PII.

Plaintiff's Injuries

27. Plaintiff suffers anxiety and mental distress due to Flagstar's failure to secure her PII, reasonably fearing identity theft resulting from the Data Breach. Plaintiff faces a heightened risk of new financial and other accounts being opened in her name, now and in the future.

28. According to the Federal Trade Commission's Consumer Sentinel Network, in 2020 there were nearly 1.4 million reports of identity theft received through the FTC's identitytheft.gov website—about twice as many as in 2019.[6] Of those reports, over 400,000 came from people who said their information was misused to apply for a government document or benefit, up from some 23,000 in 2019.[7] According to a report by Javelin Strategy & Research, identity theft cost Americans a total of about $56 billion in 2020.[8]

29. As reported in the *Detroit Free Press*, Adam Levin, founder of CyberScout and author of a book on identity theft, said, "that if criminals do publish Social Security numbers and other personal information, the victims of

[6] https://www.ftc.gov/news-events/news/press-releases/2021/02/new-data-shows-ftc-received-22-million-fraud-reports-consumers-2020 (last visited Oct. 24, 2023).

[7] *Id.*

[8] *See* https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html (last visited Oct. 24, 2023).

hacks like that affecting Flagstar customers are at high risk of tax fraud, tax refund diversion, fraudulent unemployment claims and fraudulent new account creation schemes, among other bad things."[9]

30. As a result of Flagstar's derelict data security, Plaintiff has lost the ability to control how her PII is used, and that PII has correspondingly lost value. Moreover, Plaintiff must bear additional future costs in the form of time, effort, and money to prevent, detect, contest, and/or repair the adverse effects of her PII having been stolen in the Data Breach.

31. Particularly considering Flagstar's poor track record, Plaintiff also faces a heightened risk that her PII remaining in Flagstar's possession will be compromised in the future due to the bank's inadequate cyber security policies, protocols, and procedures.

V. CLASS ACTION ALLEGATIONS

32. Plaintiff brings this lawsuit as a class action pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and/or (c)(4) on behalf the following Class and Subclass:

> **Class**
> All individuals residing in the United States whose PII was accessed or acquired by an unauthorized party in the data breach reported by Flagstar Bank on or about October 5,

[9] https://www.freep.com/story/money/business/michigan/2021/03/24/flagstar-bank-customers-information-breach-accellion/6987681002/ (last visited Oct. 24, 2023).

2023.

Michigan Subclass
All individuals residing in Michigan whose PII was accessed or acquired by an unauthorized party in the data breach reported by Flagstar Bank on or about October 5, 2023.

Plaintiff reserves the right to modify, change, or expand the Class definition, including proposing additional subclasses, based on discovery and further investigation.

Numerosity and Ascertainability

33. The number of Class Members is so large as to make joinder impracticable. The Data Breach affected approximately 837,390 individuals.

34. The identities and contact information of Class Members are readily ascertainable from information and records in the possession, custody, or control of Flagstar. Notice of this action can be readily provided to the Class.

Typicality

35. Plaintiff's claims are typical of the Class in that her sensitive personal information, like that of all Class Members, was compromised in the Data Breach made possible by Flagstar's deficient data security.

Adequacy of Representation

36. Plaintiff is a member of the proposed Class and will fairly and adequately represent and protect its interests. Plaintiff's counsel are competent

and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiff has no interest contrary to or in conflict with the interests of Class Members.

Predominance of Common Issues

37. Common questions of law and fact exist as to all members of the Class and predominate over questions pertaining only to individual Class Members. Among the questions of fact and law common to the Class are:

a. Whether Flagstar had a duty to implement reasonable cyber security measures to protect Plaintiff's and Class Members' sensitive, personal information and to promptly alert them if such information was compromised;

b. Whether Flagstar breached its duties by failing to take reasonable precautions to protect Plaintiff's and Class Members' sensitive, personal information;

c. Whether Flagstar acted negligently by failing to implement adequate data security protocols and otherwise act to secure the sensitive, personal information entrusted to it;

d. Whether Flagstar violated the Michigan Consumer Protection Act, Mich. Comp. Laws Ann. § 445.901 *et seq.*;

e. Whether Flagstar unlawfully invaded Plaintiff's and Class Members' privacy by recklessly enabling the Data Breach;

f. Whether Flagstar breached its contract with Plaintiff and Class Members by failing to fulfill its obligation to protect their PII;

g. Whether Flagstar was unjustly enriched because it acquired a financial benefit from Plaintiff's and Class Members' PII while failing to protect it;

h. Whether Plaintiff and Class Members are entitled to damages or restitution, and if so, in what amount; and

i. The propriety and form of appropriate injunctive relief.

Superiority

38. A class action is superior to all other available methods for resolving this controversy. Absent a class action, most Class Members likely would find the cost of pursuing their claims prohibitively high and would have no effective remedy. Because of the relatively small size of the individual Class Members' claims, few, if any, Class Members would seek redress for Flagstar's violations. Class treatment here will conserve judicial resources while promoting efficient adjudication and consistent results.

Generally Applicable Conduct

39. Class-wide injunctive and corresponding declaratory relief is appropriate under Rule 23(b)(2), as Flagstar acted and failed to act in a manner that applies generally to the Class.

Adjudication of Common Issues

40. Pursuant to Rule 23(c)(4), Plaintiff's claims on behalf of the Class are comprised of common issues of fact and law whose efficient adjudication in a class action will materially advance the interests of all Class Members.

FIRST CAUSE OF ACTION

Negligence

41. Plaintiff incorporates and realleges the foregoing allegations of fact.

42. Plaintiff asserts this claim on behalf of herself and the Class under Michigan law or, in the alternative, the law of the state of residence of each Class Member.

43. Flagstar collected, stored, and transferred the personal information of Plaintiff and Class Members, including their Social Security numbers, first and last names, addresses, dates of birth, and account numbers.

44. Flagstar owed Plaintiff and Class Members a duty of reasonable care to preserve and protect the confidentiality of their personal information that it collected. This duty included, among other obligations, maintaining and testing its security systems and computer networks, using up-to-date and secure versions of file transfer software, and taking other reasonable security measures to safeguard and adequately secure the personal information of Plaintiff and Class Members from unauthorized access and use.

45. Plaintiff and Class Members were the foreseeable victims of Flagstar's inadequate cybersecurity. The natural and probable consequence of Flagstar's failing to adequately secure its information networks was the hacking of Plaintiff's and Class Members' personal information.

46. Flagstar knew that Plaintiff's and Class Members' personal information was an attractive target for cyber thieves, particularly given the two major data breaches that Flagstar recently experienced. The harm to Plaintiff and Class Members from exposure of their highly confidential personal facts was reasonably foreseeable to Flagstar.

47. Flagstar had the ability to sufficiently guard against the Data Breach by implementing adequate measures to protect its systems.

48. Flagstar's duty to protect Plaintiff's and Class Members' PII also arises under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6809(3)(A) ("GLBA").

49. Flagstar is a financial institution, as that term is defined by Section 509(3)(A) of the GLBA, and thus is subject to the GLBA. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

50. Flagstar collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n), and 12 C.F.R. § 1016.3(p)(1).

Accordingly, during the relevant time period Flagstar was subject to the requirements of the GLBA, 15 U.S.C. § 6801.1 *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA statutes.

51. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau ("CFPB") became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

52. Therefore Flagstar's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

53. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous" and must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. §§ 313.4 & 313.5; 12 C.F.R. §§ 1016.4 & 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's

security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Flagstar violated the Privacy Rule and Regulation P, including because Flagstar failed to accurately disclose to its customers the true, ineffective nature of its information security and confidentiality policies and practices.

54. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and

confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein—and as the Data Breach itself demonstrates—Flagstar violated the Safeguard Rule.

55. Further, Flagstar owed Plaintiff and Class Members a duty to safeguard their PII under the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"). Pursuant to the Act, Flagstar had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ appropriate measures to protect against unauthorized access to confidential consumer data as an unfair practice that violates Section 5 of the FTC Act, 15 U.S.C. § 45(a). Orders in these actions further clarify the measures businesses must take to meet their data and cyber security obligations under the Act.

56. Flagstar breached its duty to exercise reasonable care in protecting Plaintiff's and Class Members' confidential personal information by failing to implement and maintain adequate security measures to safeguard the information, failing to monitor its systems and files to identify suspicious

activity, and allowing unauthorized access to and exfiltration of the information.

57. There is a close connection between Flagstar's failure to employ reasonable security protections for its customers' personal information and the injuries suffered by Plaintiff and Class Members. When individuals' sensitive personal information is stolen, they face a heightened risk of identity theft and need to: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries and charges; (5) place and renew credit fraud alerts on a quarterly basis; (6) contest fraudulent charges and other forms of identity theft; (7) repair damage to credit and financial accounts; and (8) take other steps to protect themselves and attempt to avoid or recover from identity theft and fraud.

58. Additionally, Flagstar owed a duty to timely disclose to Plaintiff and Class Members that their personal information had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that Plaintiff and Class Members could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax

accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) place or renew fraud alerts on a quarterly basis; (5) intensively monitor loan data and public records; and (6) take other steps to protect themselves and attempt to avoid or recover from identity theft.

59. Flagstar breached its duty to timely disclose the Data Breach to Plaintiff and Class Members. Flagstar did not inform Plaintiff and Class Members of the Data Breach until five months after it occurred. Flagstar unreasonably delayed in notifying Plaintiff and Class Members of the Data Breach. This delay caused foreseeable harm to Plaintiff and Class Members by preventing them from taking timely self-protection measures in response to the Data Breach, such as placing a credit freeze to guard against instances of identity theft.

60. The policy of preventing future harm also gives rise to an independent duty in tort on the part of Flagstar to protect the PII at issue and thereby avoid reasonably foreseeable harm to Plaintiff and the Class, particularly given the sensitive data entrusted to Flagstar.

61. As a result of Flagstar's negligence, Plaintiff and Class Members have suffered damages in an amount to be determined at trial. These damages include or may include, without limitation: (1) loss of the opportunity to control

how their personal information is used; (2) diminution in the value and use of their personal information entrusted to Flagstar; (3) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (4) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (5) unauthorized use of compromised personal information to open new financial and other accounts; (6) continued risk to their personal information, which remains in Flagstar's possession and is subject to further exposure for as long as Flagstar fails to undertake appropriate and adequate measures to protect the personal information in its possession; (7) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach; and (8) anxiety and mental distress resulting from the foreseeable and reasonable fear that they may suffer identity theft due to Flagstar's failure to adequately protect their PII.

SECOND CAUSE OF ACTION

Violation of the Michigan Consumer Protection Act, Mich. Comp. Laws Ann. § 445.901 *et seq*.

62. Plaintiff incorporates and realleges the foregoing allegations of fact.

63. Plaintiff asserts this claim on behalf of herself and the Michigan Subclass.

64. Plaintiff and Michigan Subclass Members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

65. Flagstar advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

66. Flagstar engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including: (1) representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c); (2) representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(c); (3) making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and (4) failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. §445.903(1)(cc).

67. Flagstar's unfair, unconscionable, and deceptive practices include: (1) failing to implement and maintain reasonable security and privacy measures to protect the PII of Plaintiff and the Michigan Subclass, which was a direct and

proximate cause of the Data Breach; (2) failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach; (3) failing to comply with common law and statutory duties pertaining to the security and privacy of the PII of Plaintiff and the Michigan Subclass, including duties imposed by the FTC Act, the GLBA, the Privacy Rule, Regulation P, and the Safeguards Rule, which was a direct and proximate cause of the Data Breach; (4) misrepresenting that it would protect the privacy and confidentiality of the PII of Plaintiff and the Michigan Subclass, including by implementing and maintaining reasonable security measures; (5) making partial, misleading representations that it would "protect [Plaintiff's and the Michigan Subclass's] personal information from unauthorized access and use" while omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties requiring it to reasonably protect the PII of Plaintiff and the Michigan Subclass, including duties imposed by the FTC Act, the GLBA, the Privacy Rule, Regulation P, and the Safeguards Rule; (6) omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure the PII of Plaintiff and the Michigan Subclass; and (7) omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties

pertaining to the security and privacy of the PII of Plaintiff and the Michigan Subclass, including duties imposed by the FTC Act, the GLBA, the Privacy Rule, Regulation P, and the Safeguards Rule.

68. Flagstar's representations and omissions were material because, as the representations themselves demonstrate, ensuring protection of sensitive consumer data is regarded by consumers as vitally important, including to prevent and reduce the likelihood of experiencing identity theft.

69. Flagstar's representations and omissions were likely to deceive reasonable consumers about the adequacy of Flagstar's data security and its ability to safeguard its customers' PII.

70. Flagstar intended to mislead Plaintiff and Michigan Subclass Members and induce them to rely on its partial, misleading representations and omissions.

71. Flagstar acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded the rights of Plaintiff and the Michigan Subclass.

72. As a direct and proximate result of Flagstar's unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their

bargain with Flagstar as they would not have paid Flagstar for goods and services or would have paid less for such goods and services but for Flagstar's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

73. Plaintiff and the Michigan Subclass accordingly seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, restitution, injunctive relief, and any other relief that is just and proper.

THIRD CAUSE OF ACTION

Breach of Contract

74. Plaintiff incorporates and realleges the foregoing allegations of fact.

75. Plaintiff asserts this claim on behalf of herself and the Class under Michigan law or, in the alternative, the law of the state of residence of each Class Member.

76. Plaintiff and Class Members formed a contract with Flagstar when they provided their PII to Flagstar subject to its Privacy Notice.

77. Flagstar's Privacy Notice provides detailed information about what types of customer information will be collected and shared and how that information will be protected. The Privacy Notice supplied an essential element

of the account-opening transaction and, as such, constitutes an agreement between Flagstar and individuals who provided their PII to Flagstar, including Plaintiff and Class Members.

78. Plaintiff and Class Members fully performed their obligations under this agreement with Flagstar, but Flagstar breached the agreement by failing to protect their PII.

79. Directly violating its promises to Plaintiff and Class Members in the Privacy Notice, Flagstar failed to use reasonable measures to protect their PII, resulting in its disclosure to unauthorized third parties.

80. As a direct and proximate result of Flagstar's breach of contract, Plaintiff and Class Members were damaged and deprived of the benefit of the bargain for which they rendered valuable consideration to Flagstar for its banking services.

FOURTH CAUSE OF ACTION

Unjust Enrichment

81. Plaintiff incorporates and realleges the foregoing allegations of fact.

82. Plaintiff asserts this claim on behalf of herself and the Class under Michigan law or, in the alternative, the law of the state of residence of each Class Member.

83. Plaintiff lacks an adequate remedy at law and brings this cause of

action in the alternative to her claim for breach of contract.

84. Plaintiff and Class Members conferred a monetary benefit on Flagstar by paying money for services, a portion of which Plaintiff and Class Members reasonably expected Flagstar would apply to data security measures sufficient to secure their PII. Flagstar failed to do so—and its unreasonable underfunding of information security was inequitable under the circumstances.

85. Additionally, Plaintiff and Class Members conferred a benefit on Flagstar by entrusting their PII to Flagstar. Flagstar derived profits from Plaintiff's and Class Members PII, including by using the PII to order credit reports in connection with opening their bank accounts from which Flagstar profited.

86. Flagstar unjustly enriched itself by retaining the money it reasonably should have spent on protective measures to secure Plaintiff's and Class Members' PII. Instead of ensuring an appropriate level of security that would have prevented the Data Breach, Flagstar employed cheaper, ineffective measures, directly resulting in harm to Plaintiff and Class Members.

87. Under principles of equity and good conscience, because Flagstar failed to implement appropriate data security measures mandated by industry standards, even after allowing its systems to be breached twice in the past three years, Flagstar should not be permitted to retain its ill-gotten gain, which should

instead be restored to Plaintiff and Class Members.

FIFTH CAUSE OF ACTION

Invasion of Privacy

88. Plaintiff incorporates and realleges the foregoing allegations of fact.

89. Plaintiff asserts this claim on behalf of herself and the Class under Michigan law or, in the alternative, the law of the state of residence of each Class Member.

90. Flagstar wrongfully intruded upon Plaintiff's and Class Members' seclusion. Plaintiff and Class Members reasonably expected that the personal information they entrusted to Flagstar—such as their Social Security numbers, first and last names, addresses, and dates of birth—would be kept private and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

91. Flagstar unlawfully invaded Plaintiff's and Class Members' privacy rights by:

a. failing to adequately secure their personal information from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. enabling the disclosure of personal and sensitive facts about

them without their informed, voluntary, affirmative, and clear consent.

92. A reasonable person would find it highly offensive that Flagstar, having received, collected, and stored Plaintiff's and Class Members' names, Social Security numbers, addresses, dates of birth, and other personal details, failed to protect that information from unauthorized disclosure to third parties.

93. In failing to adequately protect Plaintiff's and Class Members' personal information, Flagstar acted knowingly and in reckless disregard of their privacy rights. Although Flagstar experienced two data breaches within three years prior to the Data Breach, it nevertheless failed to upgrade its cybersecurity to a sufficient and effective level. Flagstar knew or should have known that its ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiff's position.

94. Flagstar violated Plaintiff's and Class Members' common law right to privacy, which includes the right to control their personal and private information.

95. Flagstar's unlawful invasions of privacy damaged Plaintiff and Class Members. As a direct and proximate result of these violations, Plaintiff and Class Members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully seeks an Order:

A. Certifying this case as a class action, appointing Plaintiff as Class representative, and appointing Plaintiff's counsel to represent the Class;

B. Entering judgment for Plaintiff and the Class;

C. Awarding Plaintiff and Class Members appropriate damages or restitution;

D. Ordering appropriate injunctive relief;

E. Awarding pre- and post-judgment interest as prescribed by law;

F. Awarding reasonable attorneys' fees and costs as permitted by law; and

G. Granting such further and other relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: October 26, 2023

Respectfully submitted,

/s/ *Michael N. Hanna*

Michael N. Hanna (P81462)
MORGAN & MORGAN, P.A.
2000 Town Center, Suite 1900
Southfield, MI 48075
(313) 739-1950
mhanna@forthepeople.com

Adam E. Polk (CA State Bar No. 273000)
Jordan Elias (CA State Bar No. 228731)
Simon Grille (CA State Bar No. 339009)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
(415) 981-4800
apolk@girardsharp.com
jelias@girardsharp.com
sgrille@girardsharp.com

Attorneys for Plaintiff